UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
09/281,042	03/30/99	AGURO S	TIJ-26495

023494 TM31/1024
TEXAS INSTRUMENTS INCORPORATED
P O BOX 655474, M/S 3999
DALLAS TX 75265

EXAMINER	
JONES,H	
ART UNIT	**PAPER NUMBER**
2123	8

DATE MAILED: 10/24/00

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

Office Action Summary

Application No.	Applicant(s)
09/281,042	Aguro
Examiner	**Group Art Unit**
Hugh Jones	2763

☒ Responsive to communication(s) filed on *Mar 30, 1999*

☐ This action is **FINAL.**

☐ Since this application is in condition for allowance except for formal matters, **prosecution as to the merits is closed** in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11; 453 O.G. 213.

A shortened statutory period for response to this action is set to expire *3* month(s), or thirty days, whichever is longer, from the mailing date of this communication. Failure to respond within the period for response will cause the application to become abandoned. (35 U.S.C. § 133). Extensions of time may be obtained under the provisions of 37 CFR 1.136(a).

Disposition of Claim

☒ Claim(s) *1-3* is/are pending in the applicat

Of the above, claim(s) _____ is/are withdrawn from consideration

☐ Claim(s) _____ is/are allowed.

☒ Claim(s) *1-3* is/are rejected.

☐ Claim(s) _____ is/are objected to.

☐ Claims _____ are subject to restriction or election requirement.

Application Papers

☐ See the attached Notice of Draftsperson's Patent Drawing Review, PTO-948.

☒ The drawing(s) filed on *Mar 30, 1999* is/are objected to by the Examiner.

☐ The proposed drawing correction, filed on _____ is ☐ approved ☐ disapproved.

☒ The specification is objected to by the Examiner.

☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

☒ Acknowledgement is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).

☒ All ☐ Some* ☒ None of the CERTIFIED copies of the priority documents have been

☒ received.

☐ received in Application No. (Series Code/Serial Number) _____.

☐ received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

*Certified copies not received: _____

☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

Attachment(s)

☒ Notice of References Cited, PTO-892

☐ Information Disclosure Statement(s), PTO-1449, Paper No(s). _____

☐ Interview Summary, PTO-413

☐ Notice of Draftsperson's Patent Drawing Review, PTO-948

☐ Notice of Informal Patent Application, PTO-152

--- SEE OFFICE ACTION ON THE FOLLOWING PAGES ---

DETAILED ACTION

Information Disclosure Statement

1. Applicant has referred to *scan test circuits* and *ICE systems* in the *Backround of the Invention*, but has not provided an IDS. The Examiner is aware of and has obtained numerous examples of such teachings. Applicant has also admitted that fig. 4 represents a prior art teaching - thus, admitting that Applicant is aware of specific prior art teachings. Furthermore, Applicant's invention has been disclosed as part of IEEE Standard 1149.1. It is presumed that Applicant is of at least ordinary skill in the art and therefore is presumably aware of said standard. Is Representative aware of any other relevant prior art?

Drawings

2. Figure 4 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g). Applicant has admitted (*Backround of the Invention*) that fig. 4 represents a prior art teaching.

Specification

3. The title "*Computer System*" of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

4. The following title is suggested: "*Utilizing password registers to block Scan-Path access.*"

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless --
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

6. Claims 1-3 are rejected under 35 U.S.C. 102(b) as being clearly anticipated by Bianco et al..

7. Bianco et al. disclose a method for sensitive circuit protection with set-scan testing. They further disclose (abstract) a set/scan test capability for a circuit that includes sensitive subcircuits, but that can be latched out to prevent reverse engineering the sensitive elements. A mechanism to inhibit set/scan test access to at least some of the sensitive subcircuits is selectively actuated by a control circuit to override a normal set/scan test and inhibit set/scan access to the sensitive subcircuits. Various implementations are possible, such as fusible-link PROMs for irreversibly inhibiting set/scan access to the sensitive subcircuits after an initial non-inhibited test period, the use of encryption codes to enable repeated set/scan access to the sensitive subcircuits, and an erasable/reprogrammable mechanism for inhibiting set/scan access to programmed sets of subcircuits. The invention provides for a selectable mechanism to inhibit set/scan test access to at least some of the IC's sensitive subcircuits, and a mechanism for overriding a normal set/scan test

by actuating the inhibit mechanism for the sensitive subcircuits while permitting set/scan access to the remaining subcircuits. The security system can be designed so that, in response to an applied control signal, it either irreversibly actuates the set/scan inhibit function, or it reversibly sets an inhibit and employs an access code to reinstall set/scan for the sensitive subcircuits. Various circuit designs are available to implement the invention. The set/scan inhibit function can either be permanent, or can allow the sensitive subcircuits to be included in the set/scan test chain when a control code known only to authorized parties is externally input to the device. It can be programmable with respect to the sensitive subcircuits to which set/scan access is inhibited, in which case the inhibit program is preferably erasable and reprogrammable. A common line may be used to transmit set/scan inhibit signals to each of the sensitive subcircuits, with an inhibit latch either centrally located or distributed to each of these sensitive subcircuits, or the selection of subcircuits to be inhibited may be programmable. The inhibit function is preferably implemented by diverting a set/scan test signal away from a sensitive subcircuit to a bypass circuit, with set/scan access retained for the non-sensitive subcircuits. See *all figures*. See col. 1, line 8 to col. 3, line 8.

8. Claims 1-3 are rejected under 35 U.S.C. 102(e) as being clearly anticipated by Ragavachari.

9. Raghavachari discloses a method for enhancing security in and discouraging theft of VLSI and ULSI devices. A proposed method of reducing the theft incorporates a small amount of non-

7volatile flash memory in these devices. The flash memory contains password, device serial number and user identification information. On power-up, the device initiates an encrypted password verification session through a standard interface. If the user supplied password fails, the device's operational ports (any data or control output buses) are tri-stated, thus making the device unusable. The device serial number and user identification information are useful in determining ownership of stolen devices when recovered. See fig. 1-6; col. 2, line 60 to col. 12.

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- IEEE Standard 1149.1: see entire disclosure.

- Schulman discloses a security system which is adapted to be utilized in conjunction with a device such as an electronic calculator having solid state circuit elements formed on chips wherein the elements perform predetermined functions. The system comprises a gate formed on one of the chips for interconnecting at least two of the circuit elements in response to an enable signal. A data generator is provided and an encoding device encodes the data from the data generator as a sequence of binary signals. A reference encoder generates a preselected sequence of binary signals. A comparing device is connected to the encoding device and the reference encoder and is operable to generate and apply the enable signal to the gate when the sequence of

signals from the encoding device matches the preselected sequence of signals from the reference encoder.

- Ozdemir et al. discloses a security system and method for IC circuits has at least one additional circuit element that does not contribute toward the IC's circuit function, but inhibits proper functioning of the IC in case of an attempted copying or other unauthorized use. The identity of the additional circuit elements is disguised by forming them with the visible appearance of an apparent element but with a physical modification which is not readily visible but causes them to function in a different manner, by providing different ICs with unique control codes, or both. Physical modifications not readily visible to a copyist include very narrow open circuit cuts in metallized connection lines, preferably with a focused ion beam (FIB) or laser beam; and/or disordering the lattice structure or changing the doping level of a semiconductor region, preferably with a FIB; and/or injecting electrical charge into a semiconductor region, preferably with an electron beam. The additional elements can be formed into a control code subcircuit for the IC, with the code disguised by the use of apparent elements. ICs can be grouped into an operational ring in which control codes are transmitted serially through the ring, and the invention can be applied to a combined hardware/software system. Individual copies of the software, preferably the operating system software, contain the unique control codes required by the modified ICs and the algorithms to interact with the system hardware for the purposes of transmitting, receiving, and authenticating the control codes. See fig. 11-12 and 14.

- Guttag discloses a digital processing system including a nonvolatile memory for the storage of instructions and data where the memory contains a plurality of field effect transistors which selectively conduct current according to the electrical state of their gates and the doping of their channel regions. Also included is a central processing unit for performing operations on data connected to an information transfer bus which is in turn connected to the nonvolatile memory. The information bus is additionally connected to an external interface circuit that provides interface to external peripherals. The memory is programmed by the doping of the channel regions instead of the fabrication or nonfabrication of the gates. Therefore, data that is stored in the memory is invisible to one examining the memory itself. This allows protection to software stored in the permanently programmed memory. See fig. 2; col. 1-2.

- Curd et al. disclose overridable data protection mechanism for PLDs. See abstract; fig. 1-3; col. 1, line 45 to col. 2, line 50.

- Khu discloses user-controlled I/O switching during in-circuit programming of CPLDs through the IEEE 1149.1 TAP. See fig. 1-6; col. 4, lines 1-16

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Dr. Hugh Jones whose telephone number is (703) 305-0023.

Dr. Hugh Jones

October 22, 2000

KEVIN J. TESKA
SUPERVISORY
PATENT EXAMINER